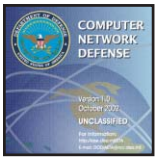
DOD Information Assurance Training & Awareness Products

Web Based Training (WBT)

NOTE: These products are web-deliverable, using html and Flash technology. They can be loaded on web servers for delivery via the Internet or intranet. As with our traditional products, they also run on a LAN or from a CD-ROM drive.



Computer Network Defense (CND)

An overview of the protection of computer systems and networks, this interactive CD-ROM details Computer Network Defense (CND) in relationship to the Global Information Grid (GIG), Network Operations (NETOPS), and Information Assurance (IA). Topics include the CND activities performed by DoD and specific CND policies that guide these activities. The user will become familiar with the overall concept of CND.

Designated Approving Authority (DAA) Basics

This interactive CD-ROM highlights the duties and responsibilities of the DAA (in industry, the Chief Information Officer (CIO) may have these responsibilities). The user will learn about members of the DAA's team, including the Information Systems Security Manager (ISSM), General Counsel, Program Manager, Information Systems Security Officer (ISSO), User Representative, and the Certification Agent. This presentation covers the Department of Defense (DOD) acquisition process, certification & accreditation (using the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) as a representation), legal and regulatory issues, and risk management. Roles of team members are discussed throughout. A glossary of terms and a resources section with relevant web sites and documents are provided for reference. The information in this product can also benefit midlevel and senior managers.

DOD Information Assurance Awareness

An updated version of DOD INFOSEC Awareness, this web based training product explains the components of Information Assurance, as well as the laws and policies designed to ensure it. In addition, DOD IA Awareness includes expanded sections to reflect the ever-changing world of information technology. Descriptions of Internal and External Threats to Information Systems, new information about technology specific vulnerabilities, and an additional focus on the Internet, including detailed discussions of email, Macro Viruses, Hoaxes, and Distributed Denial of Service (DDOS) attacks bring this product into the 21st century.

Federal Information Systems Security Awareness

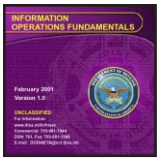
Designed specifically for users of federal computer systems, this web based training product explains the importance of Information Systems Security. Topics include: threats and vulnerabilities, malicious code, user responsibilities, and new developments affecting Information Systems Security. Non-DOD government personnel should use this product as an alternative to DOD Information Assurance Awareness.
2002 Silver AXIEM Award

Information Age Technology

Intended for those who are not Information Technology Professionals but need to understand the terms and operations of the communications infrastructure, Information Age Technology V.2.1 brings the Information Age Technology presentation into the new millennium. With an increased focus on network models and management, this course describes critical infrastructures and their relationship to the Internet. Using a transportation analogy to help students understand the behavior of networks, Information Age Technology V.2.1 provides an introduction to network hardware, such as routers, bridges, and gateways. The concepts of Uniform Resource Locator (URL), Domain Name System (DNS), Internet Protocol (IP) and "browser" functions are also discussed. Finally, an interactive email exercise allows students to use several of the concepts presented.

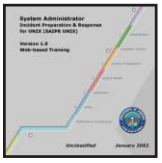
Information Assurance in Defense in Depth

Based on the Joint Vision 2020 concept of Information Superiority, and intended for military and civilian personnel responsible for the defense of DOD computers and computer networks, this web based training product explains the concept of "Defense in Depth." Using the multi-dimensional defenses of a mediaeval castle as a model, this presentation demonstrates the importance of a layered defense, which integrates the capabilities of People, Operations, and Technology. The user will learn how to defuse, detect, and react to a wide range of threats to networks, enclave boundaries, local computing environments, infrastructure support, and emerging technology.



Information Operations (IO) Fundamentals

IO Fundamentals provides an overview of IO in the joint context throughout the range of military operations. It addresses IO principles relating to both offensive and defensive IO and describes responsibilities for planning, coordinating, integrating, and deconflicting joint IO. This product is based on Joint Publication 3-13, "Joint Doctrine for Information Operations." IO Fundamentals is an update and expansion of INFOWAR Basics.



System Administrator Incident Preparation & Response for UNIX

This web based training product teaches users to prepare for and respond to information systems security incidents from a generic law enforcement perspective. Topics covered include: computer crimes, system preparation, logs and auditing, defensive tools, intrusions, and response notification and record maintenance. SAIPR UNIX is designed for individuals with three to five years of experience as System Administrators (SAs) or Information Systems Security Officers (ISSOs), and is follow up training to "UNIX Security for System Administrators."

Secret and Below Interoperability (SABI)

This product explains SABI, a network-centric process that incorporates risk management into all decisions for secret and below connectivity. It discusses the core functions and goals that have been established for the SABI process. The roles and responsibilities of the SABI community are addressed in detail.

UNIX Security for System Administrators

This product provides a basic understanding of UNIX Security. It is designed to help the beginning to inter-mediate-level administrator understand what makes up a secure UNIX system, what tools exist to protect the system, and provide assistance in the day to day tasks of monitoring and securing the network. At the completion of this course, the user will understand different UNIX environments and their origin, various UNIX threats and appropriate countermeasures, and basic encryption and security concepts. In addition, the user will learn fundamental system administration concepts, including basic commands, specific tools, network maps, sniffers, and network vulnerabilities. The resources section features links to relevant computer security web sites and a glossary of terms. Virtual hands-on exercises are provided throughout. While the exercises are based on Solaris, comparable commands in Linux Red Hat and HP-UX are demonstrated.

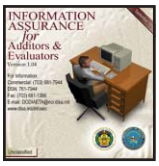
Windows NT Security

Windows NT Security details the steps necessary to safeguard system resources in a stand-alone or networked Windows NT operating environment. It provides virtual hands-on exercises to reinforce instruction of key security features. The target audience for the product is system administrators, ISSOs, and other personnel responsible for information systems administration. The user should have a basic hands-on understanding of computer systems and applications. The Resources section contains a library of Windows NT security documents to support and augment the content and exercises in the modules. There are also links to web sites related to Windows NT security.

CD-ROMs

CyberProtect

CyberProtect is an interactive computer network defensive exercise with a video game look and feel. It is intended to familiarize players with information systems security terminology, concepts, and policy. Players learn about defensive security tools, which must be judiciously deployed on a simulated network. They then face a spectrum of security threats and must make practical decisions for allocating resources (in quarterly increments) using the elements of risk analysis and risk management. Play is divided into four sessions (simulating a fiscal year). After each session, players receive feedback on how well they are doing. At the end of the last session, players are given a report detailing their cumulative operational readiness rating. The report also details every attack by type, origin, and effectiveness of defensive tools.
1999 NewMedia Gold INVISION Award (Best Overall Design)
1999 NewMedia Gold INVISION Award (Technical Training)
1999 International Cinema in Industry (CINDY) Competition Silver Award



Information Assurance (IA) for Auditors & Evaluators

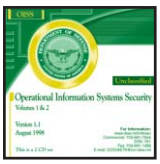
This interactive CD-ROM begins by identifying, categorizing, and detailing examples of computer crime. Topics include threats; countermeasures; confidentiality, integrity and availability; risk and risk management; and the advantages/vulnerabilities of networked systems. Laws and directives related to IA are also discussed. Overviews of certification & accreditation and the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) are encapsulated in one module. Another module addresses data reliability and integrity and includes a discussion of data testing, reporting on evidence, and key steps in assessing reliability. Finally, there is an in-depth, interactive practical exercise that allows the user to assess reliability risk, examine system controls, and determine the degree of data testing required. The user will use information presented in a fictional animated film to follow the audit trail of a rogue's missile purchases, using techniques learned in this CD-ROM. A glossary and resources section is included in this product.

Introduction to Computer Incident Response Team (CIRT) Management

This is an interactive CD-ROM intended for CIRT managers and others responsible for computer security. The user will learn how to set up and manage a CIRT, and how to handle and report computer security incidents. Procedures for hiring CIRT personnel, tools for preventing and dealing with incidents, and CIRT reporting requirements, including an explanation of IAVAs (Information Assurance Vulnerability Alerts) and INFOCONs (Information Operations Conditions), are among the topics covered. The CD-ROM also includes review exercises that highlight customer service, different types of network attacks, and incident priority.

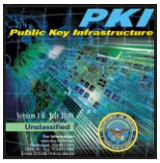
Introduction to the DOD Information Technology Security Certification & Accreditation Process (DITSCAP)

This interactive CD-ROM provides the user with an overview of the DITSCAP, including its definition, the evolution of information systems security, and roles and responsibilities. Modules 2 through 5 cover Definition, Verification, Validation, and Post-Accreditation. All modules include an overview of topics covered, a description of process activities, and individual, team, and group roles and responsibilities.



Operational Information Systems Security (OISS)

This 2 volume interactive CD-ROM set introduces the user to Operational Information Systems Security (OISS), including its definition, evolution, and legal and regulatory issues associated with information systems security. Topics include threats to information systems security, examples of security violations, incident indicators and reporting procedures, the types of trusted systems, and the certification and accreditation of systems. The roles and responsibilities of the Information Systems Security Officer (ISSO), Information Systems Security Manager (ISSM), Senior Information Systems Security Manager (SISSM), and System Design Security Officer (SDSO) are discussed. Volume 2 addresses the basics of workstation, network, and operating systems security, along with the types of storage media security. Encryption, malicious code (including its detection, prevention, and propagation), the fundamentals of risk management, and auditing goals are discussed. Users may perform exercises at the end of each module to test their comprehension. A glossary of terms is provided for reference. This product is based upon the NSA course ND225, *Operational Information Systems Security*.
1998 EMMA Award nominee



Public Key Infrastructure (PKI)

This multimedia CD-ROM introduces PKI—what it is and the security services it provides. PKI user roles are discussed, including the functions of the Registration Authority (RA), Local Registration Authority (LRA) and the End User. User Registration is covered, as well as the generation and use of certificates and keys. The Resources section has points of contact for help with PKI, including useful web sites and PKI-related documents and templates. There is also a glossary of terms for reference.

System Administrator Incident Preparation & Response (SAIPR) for Windows NT

SAIPR is an interactive multimedia training CD-ROM. It provides a virtual hands-on experience, taking the student through the steps necessary to configure networks to collect and protect event information that may be useful in an investigation of suspected unauthorized activity. The user will learn about techniques used to commit computer crimes; what information to collect prior to an incident; how to prepare systems for a possible incident; how to implement policies; how to log and recognize unauthorized activity; and how to respond to suspected unauthorized activity. Other topics covered include policies and procedures to simplify a computer emergency investigation, audit strategy, audit implementation, recognizing unauthorized activity, and notification and response strategies for security incidents. A glossary of terms and links to Service/Agency Computer Emergency Response Teams are provided for reference. This CD-ROM is a product of the DOD Computer Investigations Training Program (DCITP).

Videos

Bits & Pieces (US Govt)

This humorous video follows the exploits of Agent 000 on his bungled attempts to access proprietary information; that is until he discovers computer hacking as a means to obtain “bits and pieces” of information. (5 minutes)

Bringing Down the House (US Govt)

This video describes various hacker intrusions and how they relate to Information Warfare. The main portion of the video covers how hackers use the information superhighway to access systems. (10 minutes)

Computer Security 101 (DOJ)

John Walsh of *America’s Most Wanted* hosts this video about safeguarding computer information. Three aspects of computer security are discussed: sensitive information (what kind of information needs to be protected), risk management (reasons why computer security is important), and accountability (assuming responsibility for protecting one’s computer). (11 minutes)

Computer Security, The Executive Role (DOJ)

This video stresses the need to protect information systems at all levels of government. The user should be aware that the Office of Management and Budget (OMB) has classified all federal information as “sensitive.” To this end, steps to secure workspaces and protect data are delineated. Topics covered include the Computer Security Act of 1987, types of threats to information systems, and risk management. (9 minutes)

Dr. D. Stroye (US Govt)

This video discusses correct methods for magnetic media destruction, while providing humorous examples of how not to safely destroy data. (8 minutes)

Ears Looking at You (US Govt)

Security Officers Joe January and Frank Jones (think “Dragnet”) investigate the security vulnerabilities of cellular phones. Cellular phones act as receivers/transmitters and January and Jones know they can be a security threat to classified or proprietary information. (8 minutes)

Identity Theft: Protect Yourself

Information technology continues to alter the way in which personal information can be compromised or stolen. With the number of cases involving identity theft continuing to increase, this video assists individuals in gaining a better awareness and understanding of privacy-related issues within the private and public sectors. Topics include prevention and protection of identity information on the Internet, postal mail, and banking transactions, as well as guidance for victims of identity theft. This video also provides a variety of Internet links to many other authoritative and informative sources of privacy protection information, in addition to information on various Federal guidelines about privacy. (12 minutes)

The Information Frontline (US Govt)

This video on Defensive Information Warfare (IW-D) awareness demonstrates how information is easy to exchange but difficult to protect, the types of IW threats that exist, and the vulnerabilities of information systems. Also describes intelligence agencies that perform IW-D functions. (10 minutes)

Just the Fax, Sir (US Govt)

Security Officers Joe January and Frank Jones investigate security risks associated with the use of fax machines. As faxes are part of life in the workplace, care needs to be taken when using them to send and receive information; January and Jones help clear up the confusion. (8 minutes)

Magnificent Discretion (US Govt)

This video stresses the importance of maintaining high standards of information security, especially when working or surfing the web at home. (5 minutes)

Networks at Risk (US Govt)

This video, produced by NCS, deals with hackers, network intrusion, and computer security in the workplace. Topics covered include the selling of electronic information, prevention of network intrusions, password protection, and the importance of auditing network security. (10 minutes)

Protect Your AIS & Protect Your AIS, The Sequel (US Govt)

These videos contain INFOSEC-related dramatizations of security concerns in the workplace. These sketches demonstrate the need for password protection, virus prevention, safeguarding data, user ID security, and controlled access to computer equipment. (51 minutes)

Risky Business (NACIC, FBI)

This video warns of economic espionage and the need to protect intellectual property from hackers and corporate competitors. The film centers on a real life case of economic espionage against a Colorado firm in 1994, which ultimately led to the Economic Espionage Act of 1996.
(20 minutes) (Federal, state, local government only)

Safe Data: It's Your Job (DOL)

This video is relevant to DOD because it focuses on the need to safeguard sensitive but unclassified data, such as medical records and personnel files. It discusses ways to secure data to prevent sensitive information from getting into the wrong hands. The role of the end user in computer and network security is emphasized. Tips for preventing data from being compromised by hackers and unauthorized users, such as good password management, virus protection, and physical security are also provided. (19 minutes)

The Scarlet V (US Govt)

This video discusses the need to use virus-scanning software on a regular basis to prevent file infection. The segment parodies the life of the individual who inadvertently introduces a virus into a networked system. (7 minutes)

Sherman on My Mind (US Govt)

This humorous video examines the issue of personal projects at the workplace. As they each waste time with personal projects, four different employees are reminded of Sherman, a former employee who lost his job because of unauthorized side projects. (11 minutes)

Solar Sunrise, Dawn of a New Threat (NACIC, FBI)

This video highlights the FBI/NIPC Solar Sunrise investigation involving computer hackers who gained access to Department of Defense computers during the 1998 Iraqi weapons inspection crisis. (18 minutes) (Federal, state, local government only)

Think Before You Respond (NRO)

This video deals with Internet security, stressing the need to be careful about what information you provide over this medium. Internet users should use caution when discussing topics in live chat sessions or when responding to requests for information. (3 minutes)

Understanding PKI (DOD)

This video introduces the concept of Public Key Infrastructure (PKI) and how it can be used to ensure the security and privacy of cyber-based transactions. Topics covered include examples of how PKI works, why it is necessary to protect the DII and NII, and how it ensures the confidentiality, integrity, non-repudiation, and authentication of electronic messages through digital signatures. (13 minutes)